

DEPARTMENT OF HEALTH & HUMAN SERVICES
Centers for Medicare & Medicaid Services
7500 Security Boulevard, Mail Stop N1-19-18
Baltimore, Maryland 21244-1850



Office of Information Services

Enterprise User Administration

Users Guide

Table of Contents

Introduction.....	2
New User Requests	2
User Change Requests	2
CMS Userid Certification Requirements	3
EUA PassPort	3
Installation of PassPort	4
Logging on to PassPort	4
PassPort Home Screen	5
PassPort Certification Screens	6
Managing Passwords	10
Using PassPort to Manage Passwords	10
Setting Up Challenges.....	12
Logging on to PassPort Without a Password.....	14

Introduction

This guide provides information on the Enterprise User Administration (EUA) system used by the Centers for Medicare & Medicaid Services (CMS) and the CMS Data Center (CMSDC). The guide discusses the role of EUA in userid and password management, and provides instructions for installation and operation of EUA support products available to the user.

EUA is a system used by CMS to manage enterprise userids and passwords. It allows for centralized administration of userids on the entire CMS enterprise including the mainframe systems, mid-tier devices such as AIX or SUN systems, network operating systems such as Netware or Windows, and database platforms such as Oracle, Sybase, and MS SQL. The system utilizes online data to automate the approval process for access requests, and provides logging and auditing support.

EUA only manages resources resident at the CMSDC and at CMS Web sites. Therefore, it does not control remote dialup access userids provided by AGNS, or Health and Human Services (HHS) provided resources such as the Integrated Time and Attendance System (ITAS) and the new Email system. Users need to manage those userids and passwords through mechanisms provided in those environments. EUA also does not manage local IDs created in application tables. Users need to contact application owners for instructions on how these can be maintained.

New User Requests

The process for new users requesting access to CMS resources requires submission of a signed paper request form. For CMS employees, the new user provisioning process is handled by the agency personnel department. New contractor personnel need to complete the Application for Access to CMS Computer Systems Form available at

<http://www.cms.hhs.gov/mdcn/hdcidform.asp>

The contractor should forward the signed form according to the instructions provided with it.

User Change Requests

All users may submit change requests by sending an email to the RACF Group Administrator (RGA) responsible for their userids. The RGA will enter the request into EUA, where it will be routed to the appropriate approving authorities. Contractors must immediately notify CMS upon termination of any employees who hold CMS userids.

CMS Userid Certification Requirements

CMS requires everyone who has an enterprise userid to complete an annual certification of their access needs, and to take a security Computer Based Training (CBT) course. Users who do not complete these tasks by their certification due date will have their access rights revoked.

Six weeks prior to the due date, each user receives an email message notifying them of the need to certify and complete the CBT. The email contains Web browser links to the EUA PassPort application, and to the CBT Web pages. A printed letter is sent to those users who do not have email addresses on file with CMS. Some external users may not be able to access the PassPort and CBT services. These services are not available from the Internet, but are accessible over the Medicare Data Communications Network (MDCN). The user notifications also include instructions on using the existing paper based certification process, and an alternate CBT process.

Two weeks before the due date, a reminder notice is sent to those users who have not completed the certification requirements. If the users do not certify before the deadline, their access rights are revoked.

Users whose access rights have been revoked due to non-certification need to request reinstatement by sending an email to CMSEUA@cms.hhs.gov. If the user is a CMS employee, the request should come from their supervisor. For all other users, the RGA or project officer for the contract should send the request. Reinstatements will only be granted for a two week period. If the user does not complete the certification within the two week period, the userid will again be revoked.

Note that both the paper and electronic certifications require CMS approval before the user is considered certified. Please allow some time for this approval process, i.e., don't wait until the day before expiration to submit the certification request.

EUA PassPort

PassPort is a Web based application used to provide users with an interface to EUA. The two principal uses of PassPort are for the annual user certification of access requirements, and password management. Use of PassPort is not required by CMS, but its capabilities should simplify the userid management process for users.

Installation of PassPort

Since PassPort is a Web based application, no user installation is needed. The only software needed on the user workstation is a Web browser such as Internet Explorer or Netscape. CMS employees have an icon for PassPort on their desktops. The icon



contains the PassPort logo:

Other users can create a desktop icon for PassPort. Instructions for creating icons are available in the CMS Remote Access Guide, available at

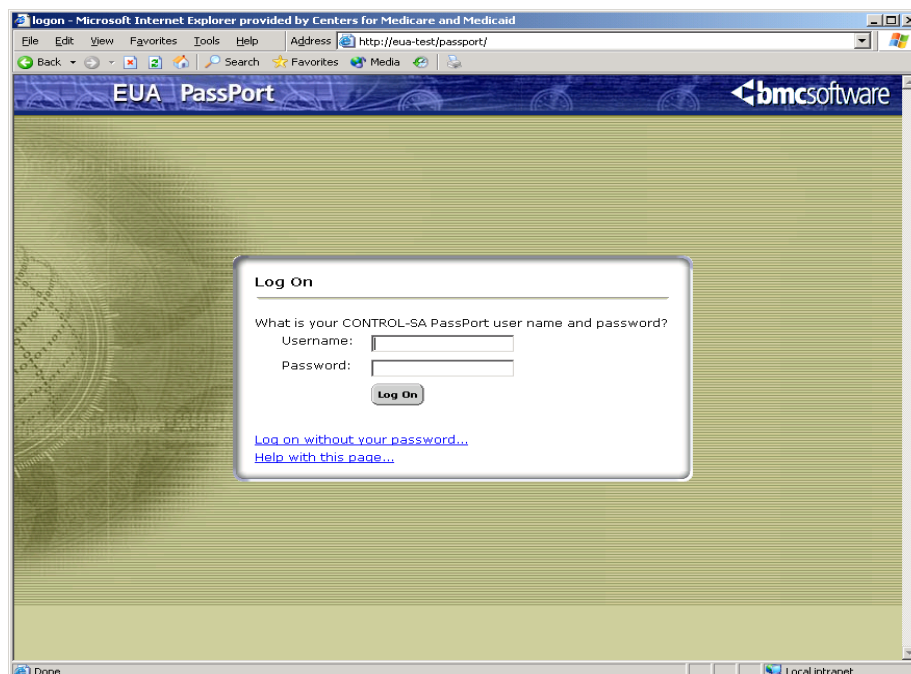
<http://www.cms.hhs.gov/mdcn/cmsremoteaccessguide.pdf>

Logging on to PassPort

PassPort is accessed by entering the following URL in the Web browser:

<https://158.73.79.141/passport>

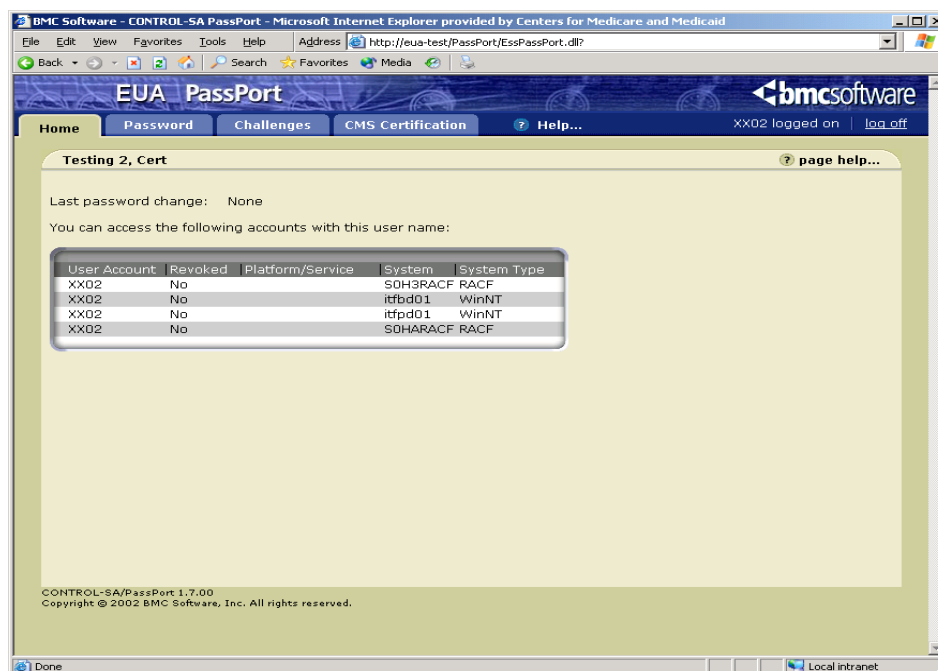
The user then enters their CMS enterprise userid and password on the following screen:

A screenshot of a Microsoft Internet Explorer browser window. The title bar reads "logon - Microsoft Internet Explorer provided by Centers for Medicare and Medicaid". The address bar shows "http://eua-test/passport/". The page has a blue header with "EUA PassPort" on the left and the "bmcsoftware" logo on the right. The main content area has a green background with a faint globe pattern. In the center is a white "Log On" box. Inside the box, it asks "What is your CONTROL-SA PassPort user name and password?". There are two input fields: "Username:" and "Password:". Below the fields is a "Log On" button. At the bottom of the box are two links: "Log on without your password..." and "Help with this page...". The status bar at the bottom shows "Done" and "Local intranet".

Users wanting to use PassPort during the initial release of EUA (June 2004) will need to initiate a password change on Netware, the mainframe, or Metaframe prior to using the product. This change is needed to synchronize PassPort's password with the rest of the enterprise. This requirement does not apply to new userids, or to those users who wait until after their normal password change cycle takes place (up to 60 days) before using PassPort.

PassPort Home Screen

Upon successful login to PassPort, the user is presented with the home screen:



This screen lists the systems on which the user has accounts, and the status of those accounts.

PassPort Certification Screens

Selecting the CMS Certification tab brings up the following screen:

CMS Certification As of Date : 2/19/2004

User Details	
User ID	XX04
User Name	Testing 4, Cert
Common Name	
Telephone Number	410-786-5801
Company Name	
Company Phone Number	
Address	
Mail Stop	n1-19-18
Desk Location	n1-19-17
Email Address	itfadmin@cms.hhs.gov

To change your user information, contact your RGA. [Click here to find the RGA for your Organization](#)

System Access Status				
OK	DUE	TEMP	PENDING	DUE DATE
				01/31/2004

To Certify your System Access click here : [Update System Access](#)

CBT Status			
OK	DUE	TEMP	DUE DATE
			01/31/2004

The screen has three sections. The first section presents the user details, as recorded in EUA. If any of this information is incorrect, the user's RGA should be contacted. The link "[Click here to find the RGA for your organization](#)" is available to assist users in finding their RGA.

The second section displays the System Access Status. In this example, the user is due for certification, and the due date is 1/31/2004. The third section displays the security CBT status. The example shows this as "DUE", with a due date of 1/31/2004.

EUA Users Guide

To certify system access, the user should click on Update System Access, at which time the following screen is presented:

Certify System Access

1. Review each System Access that is presented
2. For each System Access select either keep or delete
3. Select Certify when you are finished or select Cancel to quit

Keep : Select to retain system access to perform your current job function

Delete : Select to remove system access if access is no longer required

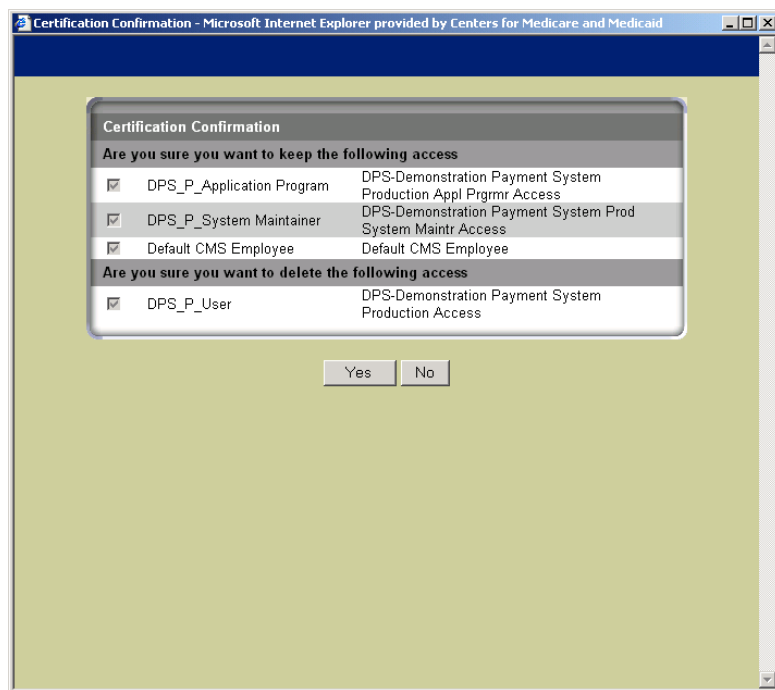
KEEP	DELETE	SYSTEM ACCESS	DESCRIPTION
<input checked="" type="radio"/>	<input type="radio"/>	DPS_P_Application Program	DPS-Demonstration Payment System Production Appl Prgmr Access
<input checked="" type="radio"/>	<input type="radio"/>	DPS_P_System Maintainer	DPS-Demonstration Payment System Prod System Maintr Access
<input type="radio"/>	<input checked="" type="radio"/>	DPS_P_User	DPS-Demonstration Payment System Production Access
<input checked="" type="radio"/>	<input type="radio"/>	Default CMS Employee	Default CMS Employee

Comments :

This screen summarizes the accesses the user holds. The user is given the opportunity to select “KEEP” or “DELETE” for each access. The comments box may be used for any comments the user wishes to provide.

EUA Users Guide

When the user has made a selection for each access, “Certify” is selected, and the following confirmation screen is displayed:



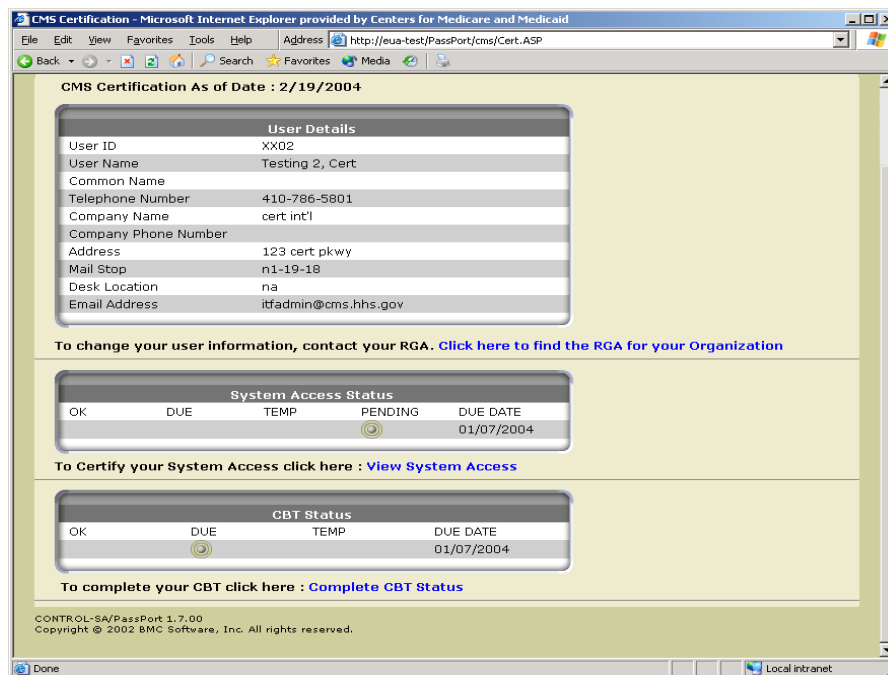
The image shows a 'Certification Confirmation' dialog box within a Microsoft Internet Explorer window. The dialog box has a title bar that reads 'Certification Confirmation - Microsoft Internet Explorer provided by Centers for Medicare and Medicaid'. It contains two sections: 'Are you sure you want to keep the following access' and 'Are you sure you want to delete the following access'. Each section has a list of access types with checkboxes. The 'Yes' and 'No' buttons are at the bottom.

Are you sure you want to keep the following access	
<input checked="" type="checkbox"/>	DPS_P_Application Program DPS-Demonstration Payment System Production Appl Prgmr Access
<input checked="" type="checkbox"/>	DPS_P_System Maintainer DPS-Demonstration Payment System Prod System Maintr Access
<input checked="" type="checkbox"/>	Default CMS Employee Default CMS Employee

Are you sure you want to delete the following access	
<input checked="" type="checkbox"/>	DPS_P_User DPS-Demonstration Payment System Production Access

Yes No

Selecting “Yes” completes the certification process for the user. At this time, the Certification screen changes the status to “PENDING”:




The image shows the 'CMS Certification' screen in a Microsoft Internet Explorer window. The address bar shows 'http://eua-test/PassPort/cms/Cert.ASP'. The page title is 'CMS Certification As of Date : 2/19/2004'. It contains several sections: 'User Details', 'System Access Status', and 'CBT Status'. The 'System Access Status' section shows a table with columns for OK, DUE, TEMP, PENDING, and DUE DATE. The 'PENDING' column is highlighted with a green circle. Below this, there is a link to 'View System Access'. The 'CBT Status' section shows a table with columns for OK, DUE, TEMP, and DUE DATE. The 'DUE' column is highlighted with a green circle. Below this, there is a link to 'Complete CBT Status'. At the bottom, there is a footer with copyright information.

USER DETAILS

User ID	XX02
User Name	Testing 2, Cert
Common Name	
Telephone Number	410-786-5801
Company Name	cert int'l
Company Phone Number	
Address	123 cert pkwy
Mail Stop	n1-19-18
Desk Location	na
Email Address	itfadmin@cms.hhs.gov


To change your user information, contact your RGA. [Click here to find the RGA for your Organization](#)

SYSTEM ACCESS STATUS

OK	DUE	TEMP	PENDING	DUE DATE
				01/07/2004

To Certify your System Access click here : [View System Access](#)

CBT STATUS

OK	DUE	TEMP	DUE DATE
			01/07/2004

To complete your CBT click here : [Complete CBT Status](#)

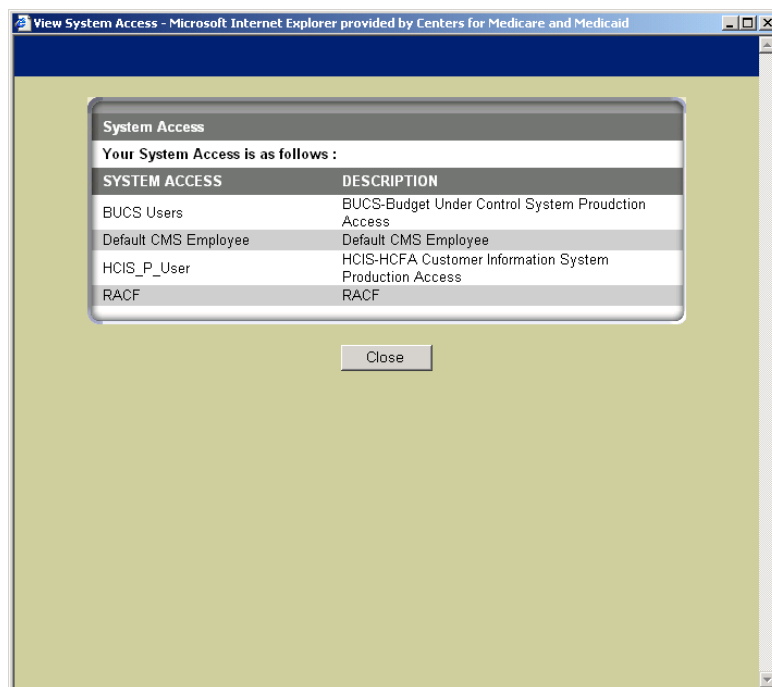
CONTROL-SA/PassPort 1.7.00
Copyright © 2002 BMC Software, Inc. All rights reserved.

EUA Users Guide

Notice that “Update System Access” has been changed to “View System Access”. The status is now set to “Pending”. It will remain in this state until the certification has been approved by CMS, at which time the status will change to “OK”.

The “Complete CBT Status” link can be selected when the user is ready to take the security CBT. Upon completion, the status will not immediately change to “OK”. The status update process for the CBT takes 24 hours.

Selecting the “View System Access” link will present the user with a summary of accesses:



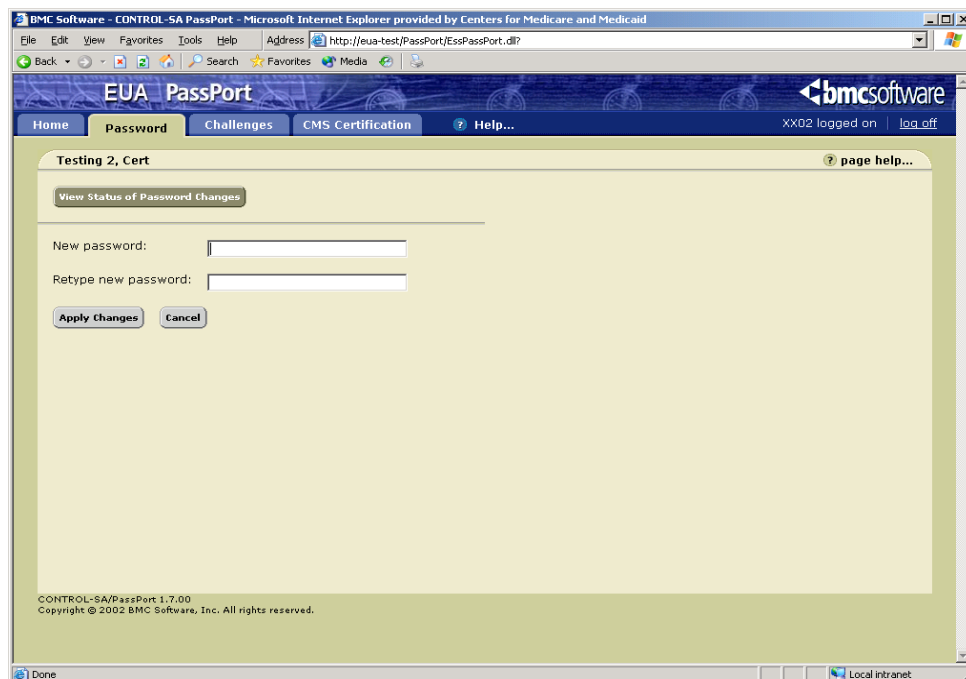
Managing Passwords

The CMS processing environment is diverse. There are hundreds of applications hosted on a variety of platforms and servers. In an effort to reduce complexity for the users, CMS has instituted Password Propagation. This is not exactly the same as Password Synchronization. In synchronization, the systems ensure that passwords are the same on all accounts. With password propagation, changes are done natively on each platform, and password interception logic on some platforms causes the password change to be propagated to all others. This means that a user can change the password on a database platform, such as Oracle or MS SQL, and that change will not affect other platforms. CMS has ensured that password changes on platforms used for initial login, namely the mainframe, Windows NT and Active Directory, Remote Desktop (Metaframe), SUN and AIX, will be propagated to all other environments, including database platforms. As long as users change their passwords on one of these initial entry platforms, or use PassPort to change their passwords, all platforms will have the same password!

Note that a password change on the Novell Netware CMS LAN environment is synchronized to Active Directory, and will therefore be propagated to all other platforms. This means that CMS employees' LAN passwords will be the same as on the other platforms.

Using PassPort to Manage Passwords

PassPort can be used to manage users' passwords. Selecting the Password tab on PassPort displays the following screen:



EUA Users Guide

The user can then type the new password, retype it for confirmation, and select “Apply Changes”. At this time, the screen will show the following:

The screenshot shows the 'EUA PassPort' web application in a Microsoft Internet Explorer browser. The user is logged in as 'L11A'. The page title is 'LITTLE, ANNE M'. The main content area displays a green checkmark and the message 'Your change request has been submitted.' Below this, there are two input fields for 'New password:' and 'Retype new password:'. At the bottom of the form are two buttons: 'Apply Changes' and 'Cancel'. The footer of the page indicates 'CONTROL-SA/PassPort 1.7.00 Copyright © 2002 BMC Software, Inc. All rights reserved.'

The status of the changes on the various platforms can be viewed by selecting “View Status of Password Changes”:

The screenshot shows the 'EUA PassPort' web application displaying the 'Status of Password Changes' page for user 'LITTLE, ANNE M'. The page includes a 'Back to change Password' button and a message: 'The following table displays the account status from the last CONTROL-SA/PassPort password change request.' Below the message is a 'Refresh Data' button and a table with the following data:

Date	Time	User Account	Platform/Service	Status
05/04/04	13:49:15	L11A		Successful
05/04/04	13:49:16	L11A		Successful
05/04/04	13:49:16	L11A		Successful
05/04/04	13:49:17	L11A.prt.NB.CO.HCFA		Successful

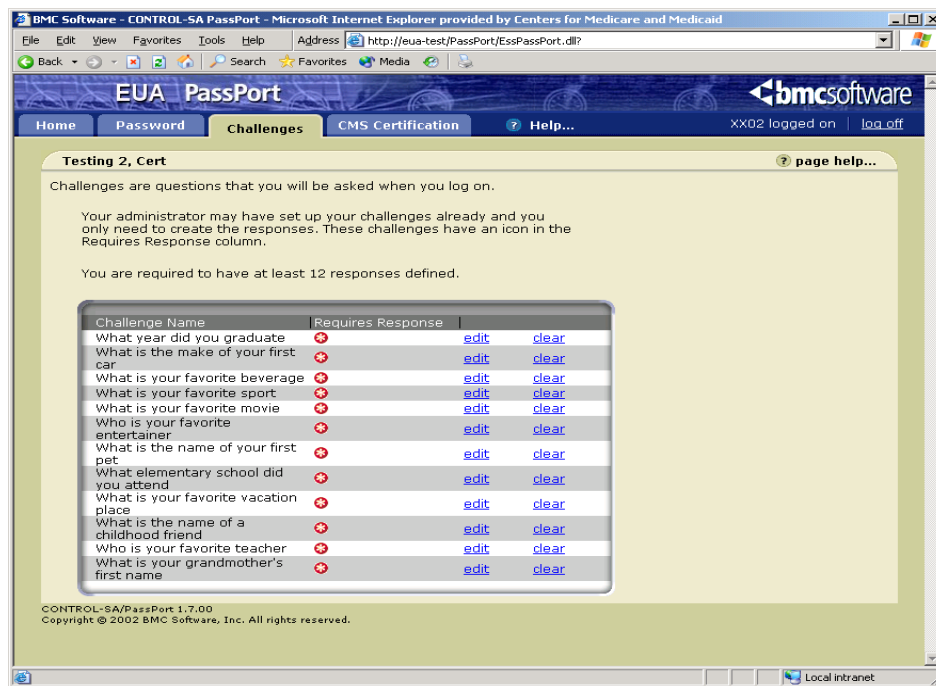
The footer of the page indicates 'CONTROL-SA/PassPort 1.7.00 Copyright © 2002 BMC Software, Inc. All rights reserved.'

The display shows the status of the password change for all accounts. The user should wait until the status is “Successful” before attempting to log on with that account.

Use of PassPort is optional. Users who cannot use PassPort, or do not wish to use it, can change their passwords when challenged by the platform and still have the change propagated to all other platforms.

Setting Up Challenges

PassPort can also be used by users who have forgotten their passwords, or who have been revoked by mistyping their passwords. In order to utilize this feature, users need to set up challenges that can be used to authenticate them prior to password reset. This is done by selecting the “Challenges” tab:



The screen contains a list of challenges for which responses are needed. To establish a response for a given challenge, the user selects “edit”.

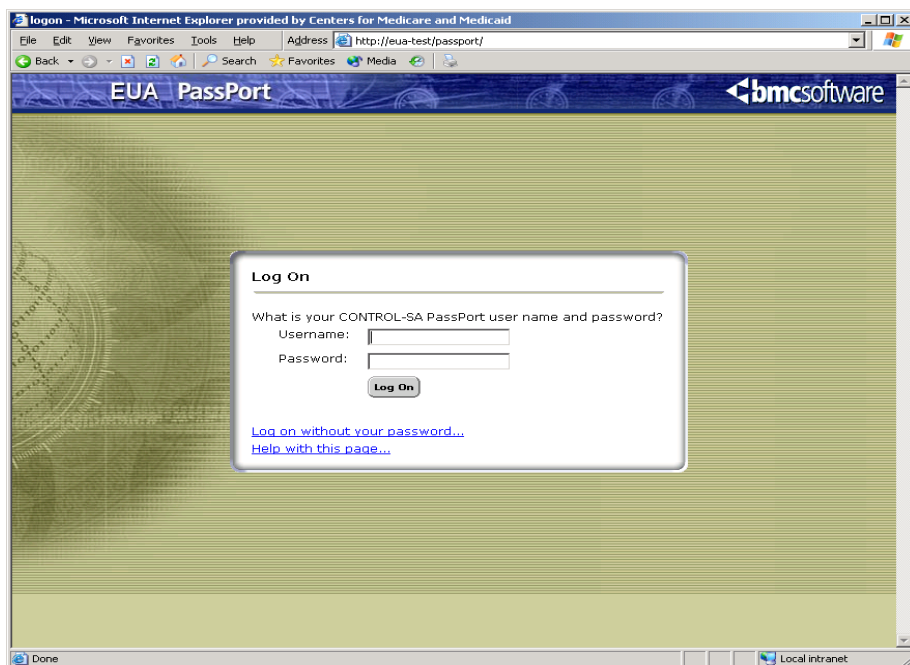
This brings up the “Edit Challenge” screen:

The screenshot shows a web browser window titled "BMC Software - CONTROL-SA PassPort - Microsoft Internet Explorer provided by Centers for Medicare and Medicaid". The address bar shows "http://eua-test/PassPort/EssPassPort.dll?". The browser's menu bar includes File, Edit, View, Favorites, Tools, Help, Address, Search, Favorites, and Media. The application's navigation bar has links for Home, Password, Challenges, CMS Certification, and Help... The user is logged in as "XX04" with a "log off" link. The main content area is titled "Testing 4, Cert - Edit Challenge" and includes a "page help..." link. A "Back to Challenges" button is at the top left. Below it, a text box explains: "Challenges are questions that you will be asked when you log on. To create or change your response to this challenge, type the response to the question, then click the 'Apply Changes' button. Your response will be updated in the list below." The challenge question is "What elementary school did you attend". The "Response:" field contains six asterisks. The "Retype Response:" field also contains six asterisks, with a note "(minimum 4 characters)". At the bottom of the form are "Apply Changes" and "Cancel" buttons. The footer of the application area reads "CONTROL-SA/PassPort 1.7.00 Copyright © 2001 BMC Software, Inc". The browser's status bar at the bottom shows "javascript:doSub('OnUpdateChallenge')", "Local intranet", and a "Local intranet" icon.

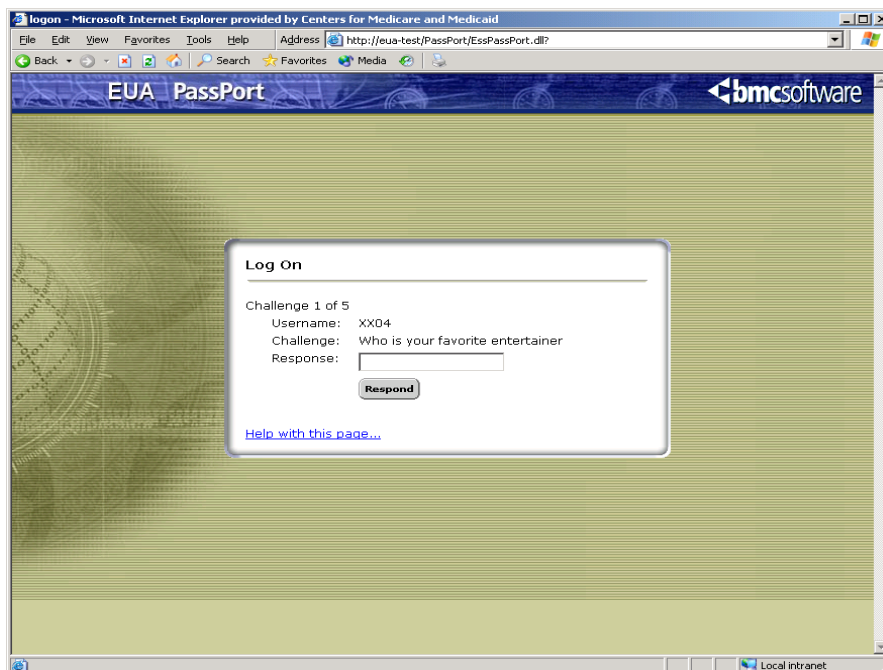
To set up the challenge, the user types and retypes the response, and selects “Apply Changes”. Responses need to be provided for all challenges. They must be a minimum of 4 characters, and the same response cannot be used for more than one challenge.

Logging on to PassPort Without a Password

Once the challenges and responses have been set up, the user can access PassPort without a password. This is done by selecting “Log on without your password” in the initial PassPort logon screen:

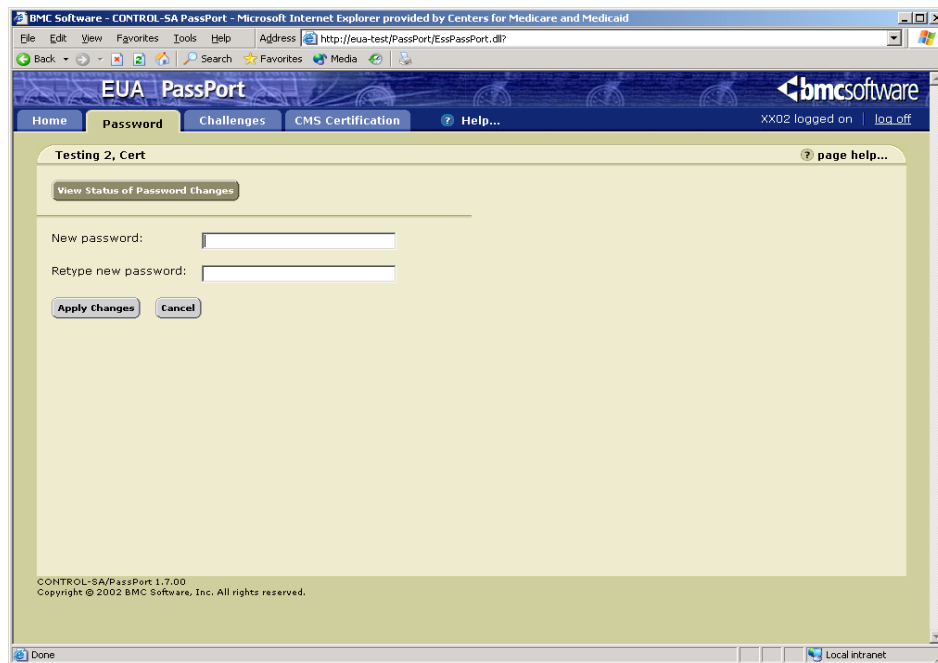


The user will be asked to provide responses to five randomly selected challenges:



EUA Users Guide

When all five are answered correctly, the user is allowed to access PassPort. At this time, the password can be changed by selecting the Password tab:



Upon completion of the password change, all user accounts are restored with the new password, and the password is valid for 60 days.

Revision History:

6/01/2004 Version 1.0